IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. JOHN CLEMENTS, Defendant.	Case No. 1:15 CR 275 **AFFIDAVIT OF TAMI LOEHRS**

I, TAMI L. LOEHRS, hereby declare as follows:

1. I am a computer forensics expert and owner of Loehrs & Associates, LLC (formerly Law2000, Inc.) a firm specializing in computer forensics. My offices are located at 3037 West Ina, Suite 121, Tucson, Arizona 85741. I am competent to testify and the matters contained herein are based on my own personal knowledge.

2. I have been working with computer technology for over 25 years and I hold a Bachelor of Science in Information Systems. I have completed hundreds of hours of forensics training including courses with Guidance Software and Access Data. I am an EnCase Certified Examiner (EnCE), an Access Data Certified Examiner (ACE), a Certified Computer Forensic Examiner (CCFE) and a Certified Hacking Forensic Investigator (CHFI). I have conducted hundreds of forensics exams on thousands of pieces of evidence including hard drives, cell phones, removable storage media and other electronic devices. I have conducted seminars on Computer Forensics and Electronic Discovery throughout the United States. In addition, I hold a Private Investigator Agency License in the State of Arizona which requires a minimum of

6,000 hours investigative experience. My Curriculum Vitae is attached hereto and updated versions may be downloaded from the Loehrs & Associates website at www.ForensicsExpert.net.

3. I have been the computer forensics expert for the defense on over 250 child pornography cases throughout the United States, Puerto Rico, Marianna Islands, Canada and England since the year 2000 and have testified over ninety times in State, Federal and international Courts.

4. I have been retained as a computer forensics expert by Ian Friedman, counsel for Defendant John Clements, for the purpose of assisting with matters related to the searching, collecting, analyzing and producing of electronic evidence in this matter.

5. I have reviewed discovery materials produced by the government including, but not limited to, Affidavits and Search Warrants, Shareaza Summary Report, Lake County Sheriff's Office Reports and Screen Shot, Property and Evidence Voucher and the Indictment.

6. According to the Affidavit prepared by Detective Seamon, this case originated from an undercover investigation of the Gnutella peer-to-peer file sharing network. On May 5, 2014, Detective Seamon downloaded four (4) complete files and three (3) incomplete files as single source downloads from IP address 99.105.84.152. That IP address was registered to AT&T Internet Services and assigned to subscriber John Clements. Detective Seamon provides no other information regarding the details of his undercover investigation such as the software and/or tools he used to download the suspect files.

7. Documents disclosed by the government include a screen shot of the Lake County Sheriff Child Protection System showing Donald Seamon logged into the system on 06/14/20 ("Screen Shot", Bates 00015). The Screen Shot depicts activity associated with IP address

99.105.84.152 and appears to be the software/tool used by Detective Seamon to conduct the undercover investigation.

8. I know from experience on numerous P2P cases and from personally listening to the testimony of law enforcement personnel, including William Wiltse, that the Child Protection System (CPS) was created at Wiltse's direction. Wiltse is or was the Director of Software Programming at TLO, a data fusion company in Boca Raton that, among other things, develops software to assist law enforcement who are investigating child exploitation crimes. CPS is a proprietary suite of software tools created by and used exclusively by law enforcement that includes software such as *ShareazaLE, Peer Spectre 2* and its predecessor *Peer Spectre*. CPS has been used by law enforcement in numerous cases throughout the country in which I have been involved as a defense expert including the matters of *United States vs. Angel Ocasio, EP-11-CR-2728(KC)* and *United States vs. John A. Crowe, 11CR 1690*. These cases, as well as others, have brought to light serious concerns with regard to the CPS software and whether that software is going beyond the scope of "publicly available" information.

9. In this case, there is particular concern regarding the ability of the CPS software going beyond the scope of "publicly available" information. The Screen Shot provided by the government includes a section titled "Keyword Searches". There are four columns of data including dates and times, keywords, an IP address, and four-digit numbers that look like port numbers. This information appears to represent keyword searches conducted by a computer at the suspect IP address that was captured by the CPS software. Additionally, based on information I recently received on another case in which I have been hired as a computer forensic consultant (United States vs. Justin Hart, Case 3:14-cr-05507-RBL), the CPS software has the ability to capture "key strokes" from a suspect computer to determine what a user is

searching for (ECF No. 41, filed 09/04/15). According to Wikipedia, *Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.* This type of data is not publicly available information, is not knowingly shared by the user and cannot be obtained with any commercially available P2P file sharing software that I am aware of.

10. On November 3 and 4, 2015, an independent forensics examination was conducted on the evidence seized from Mr. Clements' residence. Although the files identified by Detective Seamon during the undercover investigation were not found on any of the evidence items seized from Clements' residence, text fragments were located on one evidence item indicating the files existed at one time. However, I have been unable to determine if those files were publicly available at the time they were identified by Detective Seamon and the CPS software. In the Screen Shot provided by the government, SHA1 values for two of those files are identified under "Peer Logger – ShareazaLE Auto-download completed" with a date of 05/06/14. This raises further questions regarding Detective Seamon's statements in the Affidavit for Search Warrant that *he* downloaded these files on *05/05/14*.

11. It is critical to Mr. Clements' defense to understand how the CPS software functions in order to determine its reliability and accuracy in identifying files and other information reported as "publicly available" from Mr. Clements' computer. To my knowledge, as of the writing of this Affidavit, the CPS software has never been formally tested and/or validated by anyone and is unavailable for testing by any third-parties. Although the courts in *Crowe* and *Ocasio* agreed to third-party testing of the software, both cases were settled before testing could be done and the software was never made available to me.

12. For all of the reasons stated above, and under general scientific principles, it is my opinion that law enforcement's proprietary CPS software needs to be tested by a qualified third-party to determine its functionality, accuracy and its ability to go beyond the scope of "publicly available" information

13. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Dated: November 19, 2015

_____

Tami L. Loehrs